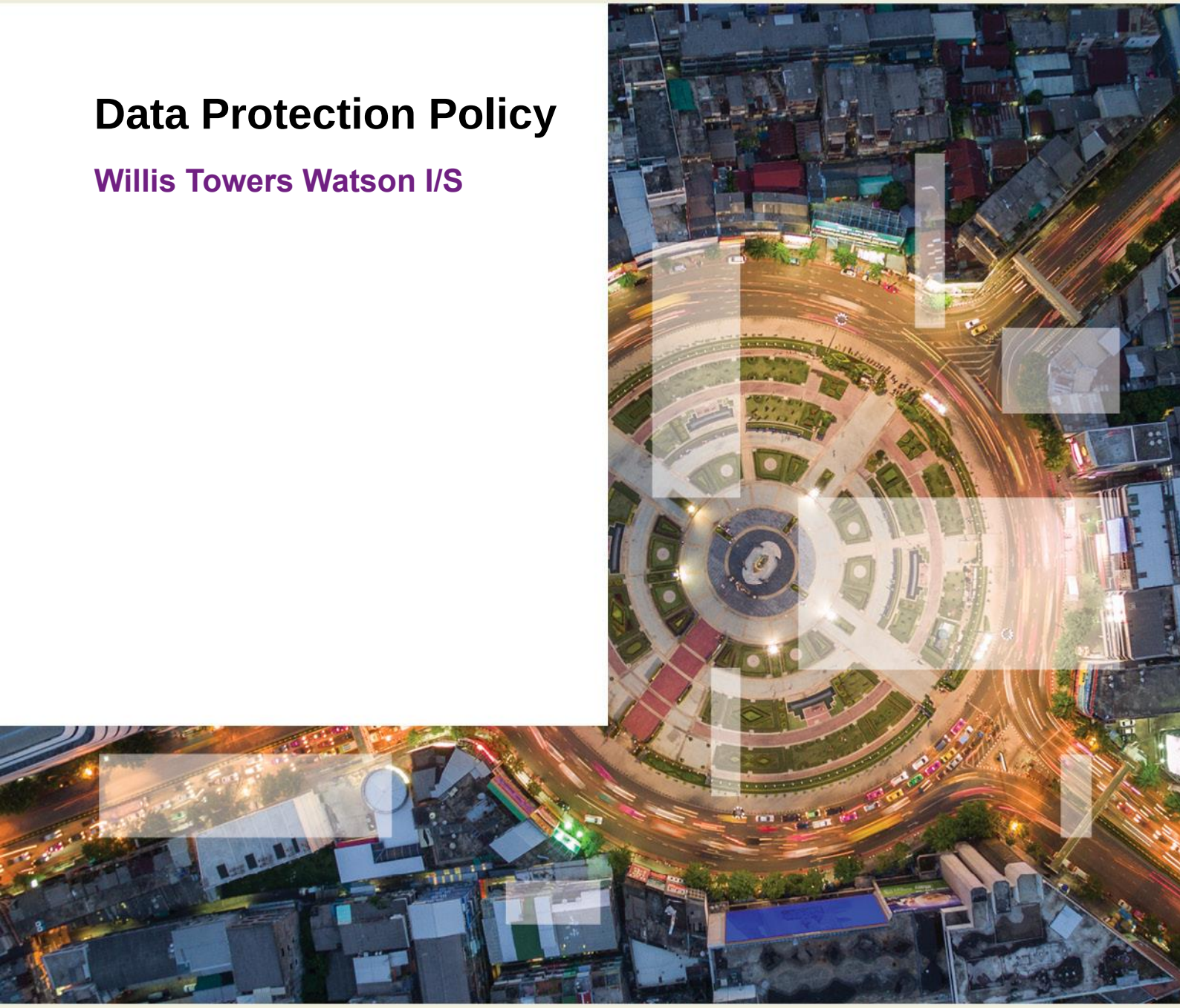
Willis Towers Watson

Data Protection Policy

Willis Towers Watson I/S



November 2020

Content

1. Introduction

1.1. This data protection policy defines the overall principles for how we collect and process personal data at Willis Towers Watson I/S (hereinafter “we” or “the Company”).

1.2. We take the protection of personal data on our clients, our clients’ employees, our own employees as well as other persons, with whom we have relations, seriously. Those who submit their personal data to us should be confident that we take care of their data and that we adhere to all current legislation on the processing of personal data.

1.3. It is vital to us that we, our management and our employees, suppliers and collaboration partners, who process data on our behalf, familiarise themselves with and adhere to the guidelines in this policy.

2. Accountability

2.1. To us it is a basic requirement to always ensure that our processing of personal data takes place pursuant to the rules on processing of personal data to which we are subject, including, but not limited to, the Data Protection Regulation (EU Regulation 2016/679) and the Danish Data Protection Act, hereinafter “the Data Protection Legislation”.

2.2. We have set up our business and business activities so that we can adhere to the Data Protection Legislation and are able to demonstrate that our processing of personal data complies with the Data Protection Legislation.

2.3. We prioritise personal data protection as one of our most significant values and we incorporate data protection principles when planning, and as a standard for, our business activities. This means that we limit our collection and processing of personal data to what is necessary and that we have implemented suitable technical and organisational measures, which ensure that we only process the required personal data to each specific purpose and that the data subjects’ rights are protected (“Privacy by design and default”).

3. Whom does the data protection policy concern?

3.1. This policy concerns all our interested parties.

3.2. The data protection policy is an addition to other instructions and policies, which we have issued, including our Information Security Policy and Archiving Policy, which establish the framework for our general IT and personal data security.

4. Who is responsible for this policy?

4.1. This data protection policy has been drawn up and approved by the management and board at Willis Towers Watson I/S.

4.2. To strengthen our data protection organisation, we have designated the Legal Department as our department responsible for personal data with the following areas of responsibility:

- Guide and assist our employees by answering queries regarding processing of personal data;
- Monitor our and our employees' adherence to this data protection policy as well as the data protection legislation in general; and
- Contact point for all external queries regarding the processing of personal data, including from those persons whose data is being processed as well as the Danish Protection Agency and other public authorities, who make sure that companies adhere to legislation.

4.3. Updated contact information can be found on our website www.willistowerswatson.com.

5. Personal data

5.1. The guidelines in this data protection policy apply to all personal data that we collect and process. Personal data is any type of data about an identified or identifiable physical person.

5.2. The data protection policy applies to all personal data

5.2.1. regardless of whether the data is submitted by the person in question or has been collected from other sources, including publicly available data;

5.2.2. regardless in which form or media the personal data is stored, including as text, picture, sound, electronically or other way;

5.2.3. regardless of whether the personal data relates to present or past clients, the clients' employees, our own employees, homepage users, persons connected to our suppliers or other business connections as well as other people with whom we have relations or on whom we process data; and

5.2.4. regardless of whether we process the data as data controller or data processor.

6. Basic principles for the processing of personal data

6.1. We, our employees and all the Company's partners must always adhere to the following basic principles on the processing of personal data:

6.1.1. We only collect and process personal data when this is legal and fair and always with the greatest amount of transparency for the person about whom we are processing data. We are open about the processing of personal data, which we carry out;

6.1.2. We only collect and process personal data for specific business reasons and legitimate and lawful purposes. If we do not have a legitimate business purpose for the processing, we will not collect it, or we will delete it;

6.1.3. We do not subsequently process data we have collected for purposes that are incompatible with the purpose of collection;

6.1.4. We only collect and process data that is required and relevant for the purposes for which we collect data. We strive to minimise the collection of data to the extent that is sufficient for the purpose;

6.1.5. We strive to ensure that the personal data we collect is correct and up to date. If we identify that personal data is incorrect, we will rectify or delete it;

6.1.6. We do not store personal data for longer time than needed. Once the purpose is exhausted and we no longer have a legitimate reason to continue to store the personal data, we delete it in a secure manner; and

6.1.7. We process personal data in a secure way and protect personal data from unauthorized disclosure – also internally – as well as against accidental loss, destruction or damage.

7. Legal basis for data processing

7.1. The Data Protection Legislation requires that personal data is collected and processed only to the extent that a relevant provision in the Data Protection Legislation can be provided. If no reference can be made, collecting and processing is illegal.

7.2. With regard to the personal data we primarily collect and process in our company, the legal basis will most often be:

7.2.1. that the person in question through his/her voluntary, specific, informed and unambiguous expression of will has given his/her consent to the processing;

7.2.2. that processing is necessary in order to enter into or fulfil a contract to which the person in question is a party;

7.2.3. that processing is necessary to comply with a legal obligation to which we are subject;

7.2.4. that processing is necessary to protect the vital interests of the person in question or of another physical person; or

7.2.5. that processing is necessary to pursue a legitimate interest unless the interest of the person in question takes precedence.

7.3. There are specific requirements to the legal basis of the processing of sensitive personal data/special categories of personal data, which include personal data on race or ethnic origin, political, religious or philosophical conviction or labour union affiliation as well as processing of genetic data, biometric data with the purpose of unambiguously identifying a physical person, health data or data on a physical person's sexual relation or sexual orientation.

7.4. Generally, we do not collect these categories of data.

7.5. However, in certain cases we may have a factual and relevant purpose with collecting data about a person's health or labour union affiliation. In those cases, we may only collect and process the data if:

7.5.1. the person in question through his/her voluntary, specific, informed and unambiguous expression of will has given his/her consent to the processing;

7.5.2. processing is necessary for us to fulfil our labour law, health law and social law obligations inasmuch that it has a legal basis in law or collective agreement;

7.5.3. processing is necessary to protect the vital interests of the person in question or of another physical person, where the person physically or legally is not capable of giving consent; or

7.5.4. processing is necessary to determine, raise or defend legal claims.

7.6. We only collect and process a person's CPR number when:

7.6.1. There is a legal basis stating that we must or may process CPR numbers, e.g. to be able to submit mandatory reports to public authorities;

7.6.2. the conditions for processing specific categories of personal data are fulfilled, cf. item 7.5; or

7.6.3. the person in question has given his/her consent.

8. Transparency

8.1. When it is appropriate or legally required, and when we collect personal data directly from individuals or clients, we will provide notice to the persons regarding what information we are collecting and the purposes for which it will be used. We will use the personal data in a manner consistent with the notice provided, unless we receive consent from the individual or the client has agreed in an applicable contract or we are required or permitted by applicable law to use it for additional purposes.

8.2. The Data Protection Legislation requires us to inform on:

8.2.1. Who we are and how we can be contacted;

8.2.2. The purposes of the processing for which we wish to collect personal data, as well as the legal basis on which we may carry out the processing (see item 7);

8.2.3. Which categories of data we process;

8.2.4. Any recipients or categories of recipients of personal data; and

8.2.5. Whether we intend to transfer personal data to a recipient outside the EEA – and if so, on what basis.

8.3. In most cases, information on the following will also need to be provided:

8.3.1. For how long we intend to process the personal data;

8.3.2. What our legitimate interests are with the processing;

8.3.3. Which rights the person in question has (see item 9);

8.3.4. Where we received the data from (when not collected from the individual), including whether the data is from publicly accessible sources; and

8.3.5. Presence of automatic decisions (without human intervention).

8.4. The information will be given concurrently with the collection of the data from the individual and within a reasonable time frame when the data is collected from another source.

8.5. There are exceptions to the obligation to inform but we only make use of these exceptions when approved by the Data Protection Officer.

9. Rights of the persons on whom we process data

9.1. Persons on whom we process data have a number of rights pursuant to the Data Protection Legislation. These are, among other:

9.1.1. The right to receive information regarding our collection and processing of personal data (see item 8);

9.1.2. The right to request access to the personal data we process about that person;

9.1.3. The right to have incorrect personal data rectified by us;

9.1.4. In certain situations, the right to have all or parts of their personal data deleted by us;

9.1.5. Under certain circumstances, the right to limit the processing to storage;

9.1.6. The right to have certain personal data provided to us by the person concerned in a structured, commonly used and machine-readable format and to transfer this data to another data controller;

9.1.7. The right to object to our processing of personal data, including an unconditional right to object to the processing of personal data for the use of direct marketing;

9.1.8. The right to revoke a given consent; and

9.1.9. The right to submit a complaint to the Danish Data Protection Agency.

9.2. We will assist, facilitate and support individuals in exercising their rights and respond to queries without undue delay and within one month of receipt of the query. If we receive a query from a person about whom we process data, our Data Protection Officer (Anne Patricia Rehlsdorph) will be informed and handle the query.

10. Integrity and confidentiality

10.1. Everyone at the Company is subject to confidentiality. The confidentiality also applies internally, and we do not share personal data with colleagues – nor informally – unless it is substantive, relevant and necessary in order for us to carry out our tasks.

10.2. Allocated usernames and passwords are personal and will not be shared with others. Employees are instructed in not helping others access data they do not have access to.

10.3. No one will access or in other ways familiarise themselves with personal data that the person does not need to carry out his/her tasks.

10.4. No one may process personal data in breach of a given instruction or in breach of our policies. Anyone who suspects that an instruction is in breach of the Data Protection Legislation or this policy will inform the Data Protection Officer immediately.

10.5. Everyone is bound to protect personal data against unauthorized disclosure as well as against other unauthorised or illegal processing and against accidental loss, destruction and damage.

10.6. Documents and files with personal data are stored in our protected case management systems. Personal data is not saved locally on PC's, USB-sticks or other mobile media, in inboxes or on open common drives. Printed material is shredded in a secure manner.

11. Personal data safety

11.1. Personal data is protected against unauthorised disclosure and against accidental loss, destruction or damage.

11.2. We safeguard personal data using appropriate physical, technical and organisational measures that are designed to protect it from loss, misuse, alteration, destruction, or unauthorised access regardless of where it is held on our systems. We continuously test and evaluate these safety measures as required.

11.3. Our Data Protection Officer will be contacted immediately upon identification or suspicion that personal data is not being subjected to the necessary safety measures or that the indicated minimum requirements are not being upheld.

12. Reporting breach on personal data security

12.1. We are obligated to report any breach on personal data security to the Danish Data Protection Agency within 72 hours after the breach has come to our knowledge. Security breaches, where personal data has come in the hands of unauthorised persons, may have extensive consequences for the people involved. Therefore, we are also obligated to inform the persons concerned when the breach carries a high risk for the security and rights of the persons involved.

12.2. A breach on personal data security is any incident that leads to accidental or illegal destruction, loss, change, unauthorised transfer of or access to personal data, regardless of whether this concerns transmitted, stored or in other way processed personal data.

12.3. Upon identification or suspicion of a breach on personal data security, employees are obligated to do what they can to stop or limit the breach and its consequences and to immediately inform the Data Protection Officer about the breach. Upon identification or

suspicion of breach, employees are obligated to, in any way possible, assist in stopping, reducing or in other ways handle the breach and limit possible damage. Additionally, the employees are obligated to be available to the Data Protection Officer and the contingency group so that we comply with our obligations pursuant to the Data Protection Legislation.

13. Transfer to countries outside the EEA

13.1. Transfer of personal data to countries outside the EEA requires a special basis for transfer. Transfer includes transfer to a data controller, transfer to a data processor and the fact that somebody in a country outside the EEA can access the data.

13.2. We expect that we will only exceptionally need to transfer personal data to a country outside the EEA.

13.3. If the need to transfer data to a country outside the EEA exceptionally arises, we ensure that the required basis for transfer is in place to ensure that the transferred personal data will also be processed securely in the recipient country.

13.4. A basis of transfer can consist of a) an EU Commission assessment that the country in question has established a sufficiently high protection level, or b) that an agreement has been entered into with the recipient regarding data protection, which has been approved by the EU Commission (EU Standard Contractual Clauses) or by another competent authority. Besides these cases, no information may be transferred to a country outside the EEA without the Data Protection Officer's approval.

14. Data controller and data processor

14.1. Our obligations pursuant to the Data Protection Legislation vary depending on whether we act in the role as data controller or data processor.

14.2. A data controller is the physical or legal person etc., who decides for which purposes and how personal data may be processed, including by whom the personal data may be processed.

14.3. A data processor is a physical or legal person etc., who processes personal data on behalf of the data controller. As opposed to the data controller, the data processor neither decides how nor for which purposes personal data may be processed but only processes the data on the basis of the data controller's instruction.

14.4. When we, as part of our services to our corporate clients, process data about the client's employees, including preparation of insurance analyses, preparation of tender material, consultations with the client and ongoing administration of the client's insurance matters, it is our opinion that we will most often be regarded as a data processor for the client. In this situation, we act solely on our client's instructions after which we must facilitate and manage the client's insurance and pension engagements.

14.5. However, when we carry out independent and personal counselling of the client's individual employees or other personal clients, e.g. regarding coverage needs, beneficiaries and supplemental contributions and in case of claims handling, our role will most often be that of data controller since we act as an independent adviser and thereby neither upon instruction from the client. In this situation, it is our responsibility to ensure that there is sufficient legal basis in the Data Protection Legislation for the processing of personal data, and it is our responsibility to ensure that the client has been given the information that it is entitled to pursuant to the Data Protection Legislation.

15. Data processors

15.1. We only use data processors, who can issue the required guarantees that they will implement suitable technical and organisational measures to ensure that the processing of the personal data complies with the requirements in the Data Protection Legislation and this policy.

15.2. Prior to entering into an agreement with a data processor, we will ask the data processor to describe the security measures that have been established, both at the data processor's and the sub-data processor's end, and we will ensure that it complies with the Data Protection Legislation and that the security measures are suitable with regards to the type of personal data and the nature of the processing activities.

15.3. A data processor's processing of personal data, for which we are responsible, must always be regulated by a written data processing agreement ensuring that the data processor solely acts upon our instructions, will not make use of data for other purposes and in general complies with the requirements stipulated in the Data Protection Legislation.

16. When we act in the role of data processor

16.1. When we act as data processor for our corporate clients or others, we ensure that we do not process personal data contrary to the instructions given, and we protect the client's personal data with the same strength as we protect our own.

16.2. To ensure that our data processing is in accordance with agreements that meet the requirements of the Data Protection Legislation, we have drawn up a standard data processing agreement that regulates our processing of the client's personal data in the delivery of our insurance broker services to the client.

17. Training and information

17.1. We ensure that new employees receive information on and training in adhering to the Data Protection Legislation and our policies. We regularly conduct training sessions and send information to all employees with the aim of refreshing their knowledge on personal data protection, inform about new rules and requirements and share our common experiences on

the processing of personal data so that we continue to ensure that we meet the requirements stipulated in the Data Protection Legislation.

18. Policy changes

18.1. We ensure that all changes to this policy are disseminated throughout the organisation so that all employees at any given time are informed about the latest version of the policy.